Sandia National Laboratories Statement of Capabilities
In Response to DARPA Draft BAA 99-33

Purpose of This Document

In recent weeks, several companies have approached Sandia about partnering with them on DARPA BAA 99-33. Federal regulations and DOE policy allow Sandia to partner with commercial entities on BAAs, but require that Sandia give all potential respondents to a BAA equal opportunity to access Sandia's capabilities. For this reason, when asked by a company to a partner on a BAA, Sandia is obliged to submit a broad statement of Sandia's applicable capabilities to the agency releasing the BAA. That agency, in turn, then makes this statement available to all organizations interested in responding to the BAA.

Per this guidance, Sandia is submitting this document to DARPA as its statement of capabilities relevant to DARPA draft BAA 99-33.

Sandia's Mission

As a Department of Energy national laboratory, Sandia works in partnership with universities and industry to enhance the security, prosperity, and well-being of the nation. We provide scientific and engineering solutions to meet national needs in nuclear weapons and related defense systems, energy security, and environmental integrity, and to address emerging national challenges for both government and industry.

Sandia Capabilities Relevant to the Information Assurance and Survivability BAA

Sandia National Laboratories has a long history in the assessment and protection of systems with respect their surety (safety, security, and reliability). Sandia has been extensively involved in the development of surety engineering techniques and tools in support of these system attributes for a diverse spectrum of applications. Surety-related expertise at Sandia is typically organized around specific methodologies (e.g., risk and reliability analysis) or specific technology domains (e.g., information technology or physical security sites).

In support of DARPA BAA 99-33, Sandia is able to bring a number of unique capabilities to bear on the problem of information assurance science and engineering. The purpose of this document is to introduce these capabilities to organizations interested in including Sandia as a member of their team when they respond to DARPA's BAA. As the capabilities listed here represent skills and resources drawn from a number of organizations within Sandia, points of contact for each of the various capabilities are listed and inquiring organizations are invited to contact these individuals directly. General questions about Sandia surety engineering capabilities and questions about appropriate mechanisms and other requirements for partnering with Sandia can be addressed to Dr. Laura Gilliom at 505-844-9104 or lrgilli@sandia.gov.

Information about Sandia's surety engineering work and capabilities can also be found at the following web locations:

http://www.sandia.gov/Surety/Surehome.htm

http://www.sandia.gov/E&E/risk/phyover.html

http://www.sandia.gov/archsur/

http://www.sandia.gov/his

http://www.sandia.gov/idart

http://www.sandia.gov/organization/div6000/ctr6500/ctr6500

Capability Focus Area: Information Surety Assessment and Design

Point of Contact

Rick Craft
505-844-8873
rlcraft@sandia.gov

Current Capability in this Technology:

For the last 6 years, staff in this area have researched next-generation assessment techniques for the assessment of information systems. A primary goal of this research has been the development of a "first principles" understanding of system assessment. This research has led to various concepts in the area of model-based assessment, with a particular emphasis on object-oriented and influence diagram-based techniques

The information surety area is also developing a number of cryptographic techniques for some novel problems faced by systems fielded by Sandia. One example of this is work being done in distributed key management protocols for use in systems where no central point of trust exists.

Research and Development

Current research activities include:

- **Source Code Assessment Tool (SCAT)**
  The goal of this current research effort is to produce a tool that permits an analyst to assess one or more bodies of source code within the context of the system to which the source code belongs. Using this model-based approach, the analyst can document what is understood about the system being assessed and readily trace dependencies through the entire system model (to include both software and non-software components).

- **Surety Life Cycle Systems Engineering**
  The objective of this ongoing research is to develop an integrated methodology and subsequent tool for the surety engineer that integrated the foour views of a system, namely object, functional, dynamic, and consequence. Current methodologies lack an integrated approach to address surety issues in the early design and development llife cycle phases of a system.

- **Ultra-low power Encryption**
  DOE has a number of places in which typical extreme power and bandwidth constraints render normal cryptographic techniques inappropriate for use. Sandia is researching alternative methods suited for these environments.

Relevant Accomplishments in this Area

Recent reports and products in this area include:

- **An Extensible, Object-oriented Framework for Risk and Reliability Assessment**
  (http://infoserve.sandia.gov/sand_doc/1999/991242.pdf). For the last several years we have researched approaches that permit a range of systems (human, information, or physical) to be assessed using multiple analysis methods.

- **Risk-based Assessment of the Surety of Information Systems (R-BASIS)**
  This visual analysis tool uses influence diagramming techniques to help an analyst determine the best alternative to improve the surety of

an information system based on risk probabilities and mitigators. The technique embodied in this tool is described in "Software System Risk Management and Assurance," August 1995, S. K. Fletcher, et. al., IEEE Computer Society, 1995 New Security Paradigms Workshop.

Sandia Resources

Staff

Sandia's efforts in information system surety engineering, cryptographic research and implementations, network security research, and red teaming provide a broad base of experience for research in the area of surety engineering methods. Sandia also has the in-house programming resources needed to prototype and implement tools and new ideas developed in the area of surety engineering

Facilities

N/A

Processing, Analytical and Mechanical Equipment

N/A

Capability Focus Area: Probabilistic Risk and Reliability Modeling and Analysis

Point of Contact

Greg Wyss
505-844-5893
gdwyss@sandia.gov

Current Capability in this Technology:

Sandia has been involved in the development of probabilistic risk and reliability analysis methodologies for more than two decades. The objects of these assessments have included commercial nuclear power plants, satellite launches, transportation systems, waste repositories, and computerized control systems. Similar techniques have been applied in the area of physical security analysis and nuclear weapons safety.

Research and Development

Current research activities in the area of risk and reliability analysis include:

- The modeling of systems that are subject to race conditions based on externally imposed boundary conditions
- Application of shortest path and optimality algorithms to the determination of possible high-risk adversary attack strategies on a given computer network
- Human performance, human reliability, and human factors
- The development of cut sets and risk expressions for arbitrarily interconnected networks
- The development of software to implement a variety of risk and reliability analysis algorithms
- Uncertainty analysis techniques as applied to risk and reliability analysis

Relevant Accomplishments in this Area

Recent reports and products in this area include:

- **Advanced Risk and Reliability Model Integrated Software (ARRAMIS)**
  This Windows-based tool provides an analyst with industrial strength fault tree, event tree, and uncertainty analyses along with graphical presentation of analysis results.
- **WinR**
  This Windows-based tool provides an analyst with the ability to perform sophisticated reliability, optimization, and uncertainty analysis and to view the results in graphical form.

Sandia Resources

Staff

Sandia has more than a dozen staff who are experienced in risk and reliability analysis, optimality analysis, uncertainty analysis, supply chain analysis, manufacturing statistics, and industrial engineering techniques. Skills include risk and reliability modeling and prediction, design of new systems, redesign of existing systems, optimization analyses, predictive maintenance technologies, statistical process control, and life cycle cost analyses.

Facilities

N/A

Processing, Analytical and Mechanical Equipment
N/A

Capability Focus Area: Physical Security Modeling and Analysis

Point of Contact

Dennis Miyoshi
505-845-9926
dsmiyos@sandia.gov

Current Capability in this Technology:

- **Fault Tree Analysis**
  Once an adversary scenario for attacking an information system has been identified, the scenario can be further analyzed to determine where the adversary must physically intrude to complete the scenario. Where the scenario requires the adversary to physically intrude, Sandia-developed fault tree analysis codes are then used to determine which sets of physical locations must be protected to prevent the scenario from succeeding.

- **Vulnerability Assessment Tools**
  Sandia was a co-developer of the ASSESS vulnerability assessment tool used within the Department of Energy to determine the effectiveness of physical security systems. Given input about the physical layers around assets, ASSESS can determine the optimal paths for the adversary to take.

- **Vulnerability Analysis of Components**
  For almost 30 years, Sandia has had the responsibility for evaluation of the vulnerability of commercial security products, including those designed to prevent unauthorized access to high value assets. These same products are being considered to control access to information systems.

Research and Development

Currently, Sandia is developing a risk-assessment tool for force protection, which can be adapted to this particular problem (what particular problem?). This tool considers threat information, asset data, and system vulnerabilities to help DoD commanders make risk-based decisions about force protection. This "Proof of Concept" tool considers blast effects and the effectiveness of physical security and mitigation measures. This risk assessment tool can be adapted to evaluate the effectiveness of appropriate protection features in an information system. Continuing research also is underway for the DOE on new access control concepts and products for information environments.

Relevant Accomplishments in this Area

The Sandia-developed Vulnerability Assessment tools are currently being used in the DOE to evaluate the effectiveness of security systems, and was recently recommended for use by the Gore Commission study on FAA security. Sandia has both developed, and examined vulnerabilities of, intrusion detection devices, camera systems, and access control devices (such as biometric systems). These technologies can be used to upgrade the control of access to information systems to a level significantly greater than that being provided by the use of passwords.

Sandia Resources

Staff
Sandia has a department of analysis experts trained in the development and application of vulnerability assessment tools. We also have a department devoted to access control systems and technologies, and we have staff trained in security systems engineering. As a partner in the Southwest Surety Institute, we teach courses in security systems and technologies at the undergraduate and graduate levels at Arizona State University, New

Mexico State University, New Mexico Tech, and Louisiana State University.

Facilities
Sandia has existing laboratories where testing is conducted on physical security technologies such as exterior and interior sensors, delay components, and display systems. Of special relevance to this BAA are our laboratories where development and testing are conducted on access control systems and various biometric identification devices.

Processing, Analytical and Mechanical Equipment
A wide suite of investigative equipment is being used in our facilities to support the current development and testing program. These include special test equipment; data systems to collect, process, and display performance data; and computing platforms upon which information protection concepts can be demonstrated.

Capability Focus Area: Tamper Protection Analysis and Design

Point of Contact

Keith Tolk
505-845-9014
kmtolk@sandia.gov

Current Capability in this Technology:

For many years, Sandia National Laboratories has been involved in the development and vulnerability testing of tags, seals, and tamper indicating enclosures for use in the verification of arms control treaties and other international agreements. As a result of this experience, personnel at SNL have extensive expertise in the design of these devices and methods that can be used to defeat them. Some of the same personnel have also been involved in the development of remote and unattended monitoring technologies that can be used to complement existing tamper indicating devices to compensate for some potential vulnerabilities.

This experience gives SNL a strong base on which to draw in the development of guidelines for the design, deployment, and inspection of tamper indicating devices for use in systems intended to ensure the integrity of information systems.

Research and Development

Relevant Accomplishments in this Area

Sandia Resources

Staff

Facilities
N/A

Processing, Analytical and Mechanical Equipment
N/A

Capability Focus Area: Sure Design

Point of Contact

Jim Martinez
505-844-0534
martijm@sandia.gov

Current Capability in this Technology:

A Model-integrated Approach to High Consequence System Surety

A ***modeling and analysis approach and a software tool set*** for integrated surety assessment of high consequence systems is being developed under the Defense Programs strategic business area at Sandia National Laboratories. Surety is the integration of safety, security and reliability design attributes in high consequence system design. The analysis approach aims to provide a thorough and complete assessment of the integrated surety attributes and their interdependencies from a common set of models. The overall technical approach for the technology is the development of the capability to construct ***functional and behavioral models*** of systems that capture the essential information for safety, security, and reliability analysis. These systems are best described by *what they do* rather than *what* components *they contain*. Functional and behavioral modeling is used to describe how systems function, and how different parts of a system interact. This approach to modeling and analysis can be applied to hardware, software, and hybrid (hardware and software) systems.

Research and Development

The project has developed a baseline integrated environment which incorporates key analytical and descriptive technologies for aid in certifying a design in the areas of safety security and reliability (surety). The methodology and approach facilitates tradeoffs amongst these attributes of surety. Further research and development requires incorporating new technologies (Markov Chains, Bayesian networks, Unified Modeling Language, etc..) to the baseline environment.

The approach to integrated surety modeling must also incorporate strategies for system modeling that allows efficient and complete representation of all possible system configurations, including different input-output events, system environments, scenarios, component failures, and triggering events. These types of models can quickly become intractable due to their magnitude and complexity. Improved methodologies for analyzing large numbers of system configurations (possibly 2^n, where n is the number of configurations) also need to be further developed.

Relevant Accomplishments in this Area

A baseline Windows® environment and tool set has been developed to model complex systems and automatically generate safety and reliability fault tree models which are seamlessly analyzed with COTS safety and reliability software packages. The fault trees are exhaustive in examining the entire design space for system configurations, faults and events leading to a safety or reliability concern.

Sandia Resources

Staff

Sandia has become a leader in the area of system surety for high consequence applications. The staff provides expertise in the area of high consequence design and high consequence surety assessment

Facilities

Sandia is able to provide supercomputing facilities and surety analytical

expertise.

Processing, Analytical and Mechanical Equipment
A wide suite of investigative equipment is being used in our facilities to support the current development and testing program. These include special test equipment; data systems to collect, process, and display performance data; and computing platforms upon which information protection concepts can be demonstrated.

Capability Focus Area: Network Security Analysis and Design

Point of Contact

Reynold Tamashiro
505-845-9804
rstamas@sandia.gov

Current Capability in this Technology:

Secure Networks & Info Systems and Advanced Networking Integration Departments provide system solutions to a wide variety of networking security and surety problems for government and commercial customers. Sandia's comprehensive network security approach encompasses all the elements that make up networks and provide five different services; *access, confidentiality, authentication, integrity,* and *nonrepudiation.*

Sandia's approach to secure network technology development includes:

- Modeling and simulation of complex networks
- Developing prototypes
- Field testing of innovative concepts
- Employing vulnerability analysis tools
- Employing sophisticated intrusion detection solutions
- Employing advanced ATM and wireless communications
- Fielding cryptography protocols and key management
- Developing innovative system concepts for distributing trust

Research and Development

Research being conducted in this area includes:

- **Computer Network Attack Analysis**
  We are developing a tool to analyze computer network vulnerabilities. The tool uses automatically-generated network configuration information, an attacker profile, and a library of known and/or hypothesized attacks to generate a weighted graph. This graph represents potential attack paths to a particular security breach or from a particular starting security state (e.g. insider attack). We then analyze near-optimal shortest paths to determine the set of most serious vulnerabilities. The tool could also be used as part of a simulation. The most critical research issues are algorithmic issues related to graph generation, defense placement, and automatic gathering of configuration information, and finding meaningful metrics for attack steps/paths. (The tool concept and high-level design are described in the following paper: L. Swiler and C. Phillips, "A graph-based system for network vulnerability analysis", Proceedings of the 1998 New Security Paradigms Workshop.)

- **Confidentiality in ATM Networks**
  Sandia recently designed a research prototype for an ATM encryptor that implements ATM encryption at 155 Mbps using a low-latency algorithm. Sandia also designed and implemented mechanisms for negotiating an encryption algorithm, performing end-user and encryption authentication, and exchanging encryption keys, using the ATM Forum's Security Message Exchange protocol. When used together, these mechanisms provide protection against eavesdropping and impersonating threats.

- **Secure Wireless Networks**
  The departments provide security solutions for wireless communication systems. Efficient cryptography algorithms have been implemented for low-power wireless communication systems. These cryptography

algorithms implement authentication and/or encryption based on the DES algorithm. Implementations have been done in both software and hardware. Systems have been developed that monitor for signs of radio jamming.

Sandia's expertise provides information security to wireless systems through information authentication, encryption, and integrity. Transmission security to provide low-probability of detection, source location, and jamming security can be included in systems.

- **Cyber Threat Activities**
  The departments have activities to collect and share cyber threat data among partnerships of industry and government participants investigating the protection of critical global infrastructures. Sandia participates in teaming efforts to develop software products that measure system and network vulnerabilities as well as detect intrusions. It is expected that networks will continue to face increasing sophistication in network attacks from various sources.

Sandia has experienced staff who are interested and willing to work with the latest in network security approaches, algorithms, and products in an effort to positively influence the direction of future improvements. In addition, Sandia employs commercially and internally developed hardware and software to develop these special capabilities.

Relevant Accomplishments in this Area

See Research & Development section above.

Sandia Resources

Staff
Staff working this area have expertise in systems reliability, combinatorial optimization, computer security and network security.

Facilities
Sandia has a network testbed to provide opportunities to evaluate various network protocols and security approaches. This testbed also allows us to perform validations to our simulations were applicable.

Processing, Analytical and Mechanical Equipment
N/A

Capability Focus Area: High Integrity Software

Point of Contact

Larry J. Dalton
505-844-2520
ljdalto@sandia.gov

Current Capability in this Technology:

Staff in this area have extensive experience in all phases of the software engineering life-cycle as applied to high consequence systems i.e. systems in which significant loss is associated with failure. The experience base includes nuclear weapon control systems, DoD Intelligence (surveillance) systems, and DoD GPS Precise Positioning Service systems. In addition, extensive systems engineering capabilities exist in evaluating all aspects of digital safety systems through a framework methodology developed for the Nuclear Regulatory Agency.

Research and Development

Current research activities in the area of high integrity software include:

- **Correctness Research**

  Theory, methods and tools are being developed to support the formalization of specifications, their abstraction, synthesis and transformation into executable code based on correctness preserving transformations. The goal is to construct an environment in which software for certain types of reactive systems can be designed and implemented in such a manner that ultra high-assurance in the correctness of the implementation is provided. In this context, the phrase "correctness of the implementation" means that the implementation satisfies its formal specification. See: http://www.sandia.gov/ast/

- **Systems Immunology™**
  This research area focuses on the dynamic (run-time) verification of a systems behavioral model through in-situ mathematical instantiations of behavioral models. This research includes the use of novel and diverse technology such as Micro-Electromechanical Systems as a means of isolating failure state spaces between the system and the "observer." In addition, this research focuses on the ability to "isolate/insulate" digital components or assets from unauthorized use whether malevolent or inadvertent in nature.

Relevant Accomplishments in this Area

Recent reports and products in this area include:

- **Correctness Research:**

  Publications for this area including referred journals can be found at:

  http://www.sandia.gov/ast/

- **Systems Immunology™**
  "The Recodable Locking Device," Communications to the ACM, July 1999, page 83-87

  1999 Discover Magazine Technological Innovations Award finalist in Emerging Technology category.

Sandia Resources **Staff**

Staff engaged in software development/engineering activities are in general SEI Capability Maturity Model level 3 or higher. Staff is predominately composed of BS/MS/PhD's.

Facilities
N/A

Processing, Analytical and Mechanical Equipment
N/A

Capability Focus Area: Surety Engineering and Surety Assessment Processes

Point of Contact

Perry D'Antonio
505-844-7956
pedanto@sandia.gov

Current Capability in this Technology:

Over the past 25 years, we have developed a robust process for designing and assessing nuclear weapons systems on a first-principles basis, with the intent of attaining the highest level of safety possible. During the past three years, we have been assessing the usefulness of this process for general surety programs and have concluded that the methodology is generally applicable to high consequence surety in a wide variety of forms. We have validated this contention under a variety of programs, for example in aviation safety for various branches of the FAA.

Research and Development

Current research and development activities include:

- **Training in Surety System Logic and Approaches**
  We have designed several courses that help focus on top-down views of surety systems. A pilot course was taught to Sandia, airline industry, and FAA personnel in April, 1999, and subsequent courses have been scheduled this Fall and are being prepared for the appropriate groups.

Relevant Accomplishments in this Area

Recent reports in this area include:

- **Deriving and Applying Generally Applicable Safety Principles** This paper was given at and published in the proceedings of the International System Safety Conference, Seattle, August, 1998. It illustrated the advantages of combining principle-based approaches in a synergistic, coordinated safety theme.

- **Structured Design and Assessment of Safety Principles**
  This paper was given at and published in the proceedings of the Probabilistic Safety Assessment and Management Conference, New York, August, 1998. It stressed the application of the surety process in general surety systems, and discussed the advantages in terms of "abnormal" (outside design specification) response.

Sandia Resources

Staff
Sandia's efforts in system surety engineering provide a broad base of experience for research in the area of synergistic surety engineering methods. Sandia also has the in-house resources needed to prototype and implement tools that utilize ideas developed in the area of surety engineering

Facilities
N/A

Processing, Analytical and Mechanical Equipment
N/A

Capability Focus Area: Hybrid (Subjective/Objective) Mathematical Models Supporting First-Principles Analysis

Points of Contact

Dave Carlson
505-844-8497
ddcarls@sandia.gov
J. A. Cooper
505-845-9168
acooper@sandia.gov

Current Capability in this Technology: Sandia has been involved in the development of first-principle-based probabilistic risk and reliability analysis methodologies for more than two decades. The objects of these assessments have included commercial nuclear power plants, nuclear weapons response, and aviation safety.

Research and Development Current research activities in the area of hybrid risk and reliability analysis include:

- The physical response modeling of systems that are subject to race conditions based on externally imposed environments
- The incorporation of subjective information in a hybrid mathematical structure with more conventional objective analysis
- Human performance, human reliability, in human factors
- The development of software to implement a variety of hybrid risk and reliability analysis algorithms
- Uncertainty analysis techniques as applied to hybrid risk and reliability analysis

Relevant Accomplishments in this Area Recent papers and patent disclosures in this area include:

- **Constrained Mathematics Evaluation in Probabilistic Logic Analysis**
  This paper, published in the International Journal of Reliability and System Safety, June 1998, illustrated an extremely effective solution to a little-recognized problem in obtaining accurate uncertainty analysis computations.
- **Hybrid Processing of Stochastic and Subjective Uncertainty Data**
  This paper, published in the Risk Analysis Journal in December, 1996, showed for the first time how a hybrid structure could be constructed to combine subjective and objective information in a common analysis.
- **Patent Disclosure for Organizational Safety Assessment and Display**
  This disclosure, constructed earlier this year, demonstrates a method of calculating and displaying organization-oriented data of importance to surety.

Sandia Resources

Staff
N/A

Facilities
N/A

Processing, Analytical and Mechanical Equipment
N/A

Capability Focus Area: Information Surety Assessment and Design

Point of Contact

Dr. Sharon M. DeLand
505-844-8740
smdelan@sandia.gov

Current Capability in this Technology:

Just in the past year, Sandia staff members have developed and successfully demonstrated two proof-of-concept computational tools. One tool utilizes finite state machines to monitor and track process flows. It has been recently applied to monitor the complete transfer cycle of out-of-reactor spent fuel to final disposition within dry storage silos. The proof-of-concept tool compares monitor system acquired sensor response data versus the allowable site-specific declared activities and identifies any anomalies with respect to normal activities and processes. Specifically designed to be generic and site non-specific in nature, the proof-of-concept allows an operator to describe the facility and associated processes as state machines so no further coding is required for application to a different facility.

Another recently developed tool converts and elevates raw sensor response data into observable events at a semantic level familiar to an inspector or other decision-maker. A key feature of the prototype is the ability to process response data from any discrete, analog or digital sensor by describing waveform characteristics, which generally requires only a few rules. The tool analyzes the set of sensor responses based upon the limited rule set and identifies human observable events of interest.

Research and Development

Current research and development activities include:

- **Knowledge Generation**
  Knowledge Generation (KG) is a methodology and process for analyzing and interpreting data to derive information useful for reaching conclusions and making decisions. The objective of the current research effort is to produce a computational tool that compares acquired sensor response data with declared activities, and displays the results at a semantic level appropriate to an inspector or other operational decision-maker.

- **Fuzzy Data Mining**
  Data mining is an emerging technology using artificial intelligence techniques to identify patterns in large data streams, whereas fuzzy set theory permits membership in more than one set and is useful for quantifying uncertainty or allowing alternative interpretations. We are performing research into combining the two mathematical formulations into fuzzy data mining in order to develop new pattern recognition algorithms well suited to large data streams and significantly increase our ability to detect, isolate and characterize undeclared activities.

- **Unattended Remote Monitoring System Design Methodology**
  Sandia is developing a formalized analytical methodology for the design, development, implementation and assessment of unattended monitoring systems. A systems level engineering design philosophy provides a structured approach to development of unattended monitoring systems for safeguards, non-proliferation, and transparency applications. The methodology recognizes overall system design is generally initiated by some external stimulus as an agreement or treaty, and yields an optimized monitoring system, which minimizes false signals while ensuring that events of interest are detected and

appropriately analyzed.

Relevant Accomplishments in this Area

Recent reports and products in this area include:

- **Embalse Knowledge Generation**
  Proof-of-concept prototype computational tool demonstrating unattended remote monitoring system sensor response data can be processed utilizing finite state machines.
- **Finite State Machine Analysis of Remote Sensor Data**
  Institute of Nuclear Material Management 40th Annual Meeting, July 25-29, 1999, Phoenix, AZ
- **Unattended Monitoring System Design Methodology**
  Institute of Nuclear Material Management 40th Annual Meeting, July 25-29, 1999, Phoenix, AZ

Sandia Resources

Staff
Sandia National Laboratories broad base of experience and capabilities in information system surety engineering, mathematical modeling and simulation, and model-based analysis are distributed among several organizations. Experience ranging from development of satellite ground station software to the fastest computer in the world has endowed Sandia with unique capabilities and resources directly applicable to the research and development of information assurance concepts and associated technologies.

Facilities
N/A

Processing, Analytical and Mechanical Equipment
N/A

Capability Focus Area: Real Time Decision Support Systems

Point of Contact

Bernie Clifford
(505) 284-3102
bpcliff@sandia.gov

Current Capability in this Technology:

Sandia has a history of delivery distributed information system for over 30 years. We have a history of delivering small and large strategic decision support systems for over 10 years. This has resulted in a proven track record partnering with industry and small businesses to meet government based customer needs.

Over time we have enhanced our expertise in performing theoretical and applied research for the strategic decision support systems we design and deliver. This includes developing prototypical applications and innovative solutions for our government based customers.

Research and Development

Research and development being conducted in this area include:

- Advanced data analysis techniques
- Integration of multiple analysis methodologies
- Modular based simulators
- Highly reliable, widely distributed systems
- Organizational and social cultural engineering effects on system vulnerabilities
- Usability engineering for decision support systems

Relevant Accomplishments in this Area

Designed, implemented, and supported multiple generations of highly available real-time decision support systems for both fixed and mobile facilities. These systems use multiple data sources to discern and validate national security related events as they are unfolding.

Developed simulators for generating multiple event scenarios used to test a variety of decision support systems**.**

Extensive experience with developing experimental system to validate proof-of-concepts for information centric decision support systems.

Followed up the delivery of the Comprehensive Test Band Treaty (CTBT) knowledge base with continued research deliverables in advanced analysis of multi-type sensor systems.

Designed and delivered the commander-in-chief mobile alternate headquarters (CMAH) to function as the survivable command center

Sandia Resources

Staff

Staff working in this area have expertise in distributed systems, software development, systems reliability, computer security and network security. Model developers and analysts also work with these staff to design, implement and validate system.

Our staff is also highly experienced in working side-by-side with sensor developers inside and outside Sandia to optimize the total knowledge gained as data moves from data collection to data storage and on through analysis.

Facilities

N/A

Processing, Analytical and Mechanical Equipment
N/A

Staff
Staff working in this area have expertise in distributed systems, software development, systems reliability, computer security and network security. Model developers and analysts also work with these staff to design, implement and validate system.

Our staff is also highly experienced in working side-by-side with sensor developers inside and outside Sandia to optimize the total knowledge gained as data moves from data collection to data storage and on through analysis.

Facilities
N/A

Processing, Analytical and Mechanical Equipment
N/A

Capability Focus Area:	High-Assurance Software Agent Technology
Point of Contact	Laura Gilliom (505) 844-9104 lrgilli@sandia.gov
Current Capability in this Technology:	Sandia's Advanced Information Systems Laboratory has developed an intelligent agent architecture, Standard Agent Architecture I, and has used the architecture to build a sophisticated e-commerce application prototype, the Border Trade Facilitation System. We are currently developing a second generation architecture that is customized for general use in high-consequence, multi-agent system applications. The principal focus of our research is on building a broadly useable agent-based system (i.e., not customized to a single application, but customizable for a spectrum of applications) with explicit, up front attention to the surety-- security, reliability, safety -- of the system. Our research agenda addresses issues associated with the integrity of individual agents (e.g., managing sensory input, developing introspective capability to detect tampering) and operational security issues associated with agent collectives (e.g., communications security, detecting broken or malevolent agents). We believe that the serious application of agent-based systems to national security needs such as C4I or network survivability will require a high level of attention to the surety of such systems -- and that we have developed an unparalleled capability in this area at Sandia.
Research and Development	As described above.
Relevant Accomplishments in this Area	As described above
Sandia Resources	**Staff** We have a limited number of Sandia staff working in this area, all of whom have strong expertise in artificial intelligence, distributed systems, information security, and advanced dynamic object-oriented software development. **Facilities** Sandia has a large-scale distributed computing facility, our C-plant, which contains 128 networked IBM/NT systems and roughly 450 networked DEC Alpha/Linux systems. This has proven to be a useful testbed for multi-agent systems development. **Processing, Analytical and Mechanical Equipment** N/A

Capability Focus Area: IDART

Point of Contact

Brad Wood
(505) 844-8461
bjwood@sandia.gov

Current Capability in this Technology:

Sandia has an established Information Design Assurance Red Team (IDART) program. IDART is part of Sandia's capability in the areas of information operations and surety of critical infrastructures. This program draws on our long history of independent assessment and utilized Sandia's broad base of technical and scientific staff.

IDART assessments evaluate projects and programs for system vulnerabilities in the area of information warfare, information assurance, and information surety. Assessments are intended to provide feedback for improvement of the system, to provide awareness of residual vulnerabilities, and to allow for procedural mitigation of remaining vulnerabilities.

Systems destined for future application must be evaluated by those cognizant of state-of-the-art technology and technology trends. Sandia provides the capability to model a full spectrum of threats, to appreciate and exploit the complexities of systems integration, and to develop and use innovative science and technology in support of IDART assessments. Further information is provided at http://www.sandia.gov/idart

Research and Development

N/A (contained in other capability statements)

Relevant Accomplishments in this Area

See above-referenced Web site.

Sandia Resources

Staff
A core team of information systems security experts manage all IDART projects. Domain experts, chosen to assure expertise appropriate to the specific analysis being undertaken, are accessed from throughout the Laboratories to support the core IDART team

Facilities
The team is supported by several laboratories designed for information warfare activities.

Processing, Analytical and Mechanical Equipment
N/A

Special Information Relevant to DARPA-sponsored BAA 99-33

IDART is employed by some (but not all) DARPA programs participating in BAA-33 as an independent red team to perform technology assessments. In the case where a DARPA program manager has already committed to employing IDART, IDART will not participate in proposals targeted to those programs in order to avoid the appearance of a conflict of

interest. With the exception noted above, IDART is available to provide red-team support as needed by proposing teams. Contact Brad Wood (contact information above) for any clarification needed.